UNITED STATES DISTRICT COURT
MIDDLE DISTRICT OF TENNESSEE
NASHVILLE DIVISION

ALEXANDER TIPPING, on behalf of himself and all others similarly situated,	)	
Plaintiff,	)	Case No._____
vs.	)	Jury Trial Demanded
EQUIFAX INC.,	)	
Defendant.	)	

CLASS ACTION COMPLAINT

Plaintiff Alexander Tipping ("Plaintiff"), individually and on behalf of the Classes defined below, alleges the following against Defendant Equifax Inc. ("Equifax"):

NATURE OF THE CASE

1. Plaintiff brings this class action case against Equifax for its failures to secure and safeguard consumers' personally identifiable information ("Personal Information") which Equifax collected from various sources in connection with the operation of its business as a consumer credit reporting agency, and for failing to provide timely, accurate, and adequate notice to Plaintiff and Class members that their Personal Information had been stolen and precisely what types of information were stolen.

2. Equifax has acknowledged that a cybersecurity incident (the "Data Breach") has occurred, potentially impacting approximately 143 million U.S. consumers. It has also acknowledged that unauthorized persons exploited a U.S. website application vulnerability to gain access to certain files. Equifax claims that based on its investigation, the unauthorized

access occurred from mid-May through July 2017. The information accessed includes names, Social Security numbers, birth dates, addresses, and, in some instances, driver's license numbers. In addition, Equifax has admitted that credit card numbers for approximately 209,000 U.S. consumers, and certain dispute documents with personal identifying information for approximately 182,000 U.S. consumers, were accessed.

3. Equifax has acknowledged that it discovered the unauthorized access on July 29, 2017, but has failed to inform the public why it delayed notification of the Data Breach to consumers. Instead, Equifax executives sold at least $1.8 million worth of shares before the public disclosure of the breach. It has been reported that its Chief Financial Officer John Gamble sold shares worth $946,374, its president of U.S. information solutions, Joseph Loughran, exercised options to dispose of stock worth $584,099, and its president of workforce solutions, Rodolfo Ploder, sold stock worth $250,458.

4. The Personal Information for Plaintiff and the class of consumers he seeks to represent was compromised due to Equifax's acts and omissions and Equifax's failure to properly protect the Personal Information.

5. Equifax could have prevented this Data Breach. Equifax knew there was a risk of such a breach. Data breaches at other companies, including one of its major competitors, Experian, have occurred.

6. The Data Breach was the inevitable result of Equifax's inadequate approach to data security and the protection of the Personal Information that it collected during the course of its business.

7. Equifax disregarded the rights of Plaintiff and Class members by intentionally, willfully, recklessly, and/or negligently (1) failing to take adequate and reasonable measures to

ensure its data systems were protected, (2) failing to disclose to its customers the material fact that it did not have adequate computer systems and security practices to safeguard Personal Information, (3) failing to take available steps to prevent breach from ever happening, and (4) failing to monitor and detect the breach on a timely basis.

8. As a result of the Equifax Data Breach, the Personal Information of the Plaintiff and Class members has been exposed to criminals for misuse. The injuries suffered, or likely to be suffered, by Plaintiff and Class members as a direct result of the Equifax Data Breach, include:

a. unauthorized use of their Personal Information;

b. theft of their personal and financial information;

c. costs associated with the detection and prevention of identity theft and unauthorized use of their financial accounts;

d. damages arising from the inability to use their Personal Information;

e. loss of use of and access to their account funds and costs associated with inability to obtain money from their accounts or being limited in the amount of money they were permitted to obtain from their accounts, including missed payments on bills and loans, late charges and fees, and adverse effects on their credit including decreased credit scores and adverse credit notations;

f. costs associated with time spent and the loss of productivity or the enjoyment of one's life from taking time to address and attempt to ameliorate, mitigate and deal with the actual and future consequences of the Data Breach, including finding fraudulent charges, purchasing credit monitoring and identity theft protection services, and the stress, nuisance and annoyance of dealing with all issues resulting from the Equifax Data Breach;

g. the imminent and certainly impending injury flowing from potential fraud and identify theft posed by their Personal Information being placed in the hands of criminals and already misused via the sale of Plaintiff's and Class members' information on the Internet black market;

h. damages to and diminution in value of their Personal Information entrusted to Equifax for the sole purpose of purchasing products and services from Equifax; and

i. the loss of Plaintiff's and Class members' privacy.

9. The injuries to Plaintiff and the Class members were directly and proximately caused by Equifax's failure to implement or maintain adequate data security measures for Personal Information.

10. Further, Plaintiff retains a significant interest in ensuring that his Personal Information, which, while stolen, remains in the possession of Equifax, is protected from further breaches, and seeks to remedy the harms he has suffered on behalf of himself and similarly situated consumers whose Personal Information was stolen as a result of the Equifax Data Breach.

11. Plaintiff brings this action to remedy these harms on behalf of himself and all similarly situated individuals whose Personal Information was accessed during the Data Breach. Plaintiff seeks the following remedies, among others: statutory damages under the Fair Credit Reporting Act ("FCRA"), reimbursement of out-of-pocket losses, other compensatory damages, further and more robust credit monitoring services with accompanying identity theft insurance, and injunctive relief including an order requiring Equifax to implement improved data security measures.

JURISDICTION AND VENUE

12. This Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds $5 million exclusive of interest and costs. There are more than 100 putative class members, and at least some members of the proposed Class have a different citizenship from Equifax.

13. This Court has personal jurisdiction over Equifax because Equifax regularly conducts business in Tennessee, and has sufficient minimum contacts in Tennessee. Equifax intentionally and purposely availed itself of this jurisdiction by marketing and selling products and services and by accepting and processing payments for those products and services within Tennessee.

14. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(b) as a substantial part of the events, acts, and omissions giving rise to Plaintiff's claims occurred in this District.

PARTIES

15. Plaintiff Alexander Tipping is Tennessee resident. Plaintiff resides in Davidson County, Tennessee. Plaintiff is a victim of the Data Breach. Plaintiff is a Canadian citizen with permanent resident status.

16. Defendant Equifax Inc. is a Georgia corporation with its principal place of business in Georgia. Equifax Inc. may be served through its registered agent, The Prentice-Hall Corporation System, Inc., 2908 Poston Ave, Nashville, TN 37203.

FACTUAL ALLEGATIONS COMMON TO THE CLASS

17. Equifax is one of three nationwide credit-reporting companies that tracks and rates the financial history of U.S. consumers. The companies are supplied with data about loans, loan payments and credit cards, as well as information on everything from child support payments, credit limits, missed rent and utilities payments, addresses, and employer history. All of this information, and more, factors into credit scores.

18. Unlike other data breaches, not all of the people affected by the Equifax breach may be aware that they are customers of the company. Equifax gets its data from credit card

companies, banks, retailers, and lenders who report on the credit activity of individuals to credit reporting agencies, as well as by purchasing public records.

19. According to Equifax's report on September 7, 2017, the breach was discovered on July 29th. The perpetrators gained access by "exploit[ing] a . . . website application vulnerability" on one of the company's U.S.-based servers. The hackers were then able to retrieve "certain files."[1]

20. Included among those files was a treasure trove of personal data: names, dates of birth, Social Security numbers, and addresses. Equifax states that the perpetrators gained access to the actual credit card numbers of around 209,000 U.S. consumers. The perpetrators also gained access to documentation about disputed charges. Those documents contained additional personal information of around 182,000 U.S. consumers.[2]

21. Personal data like this is a major score for cybercriminals who will likely look to capitalize on it by launching targeted phishing campaigns.

22. Plaintiff suffered actual injury in the form of damages to and diminution in the value of his Personal Information—a form of intangible property that was compromised in, and as a result of, the Equifax Data Breach.

23. Additionally, Plaintiff has suffered imminent and impending injury arising from the substantially increased risk of future fraud, identity theft and misuse posed by his Personal Information being placed in the hands of criminals who have already, or will imminently, misuse such information.

---

[1] Equifax Press Release (September 7, 2017), available at: http://www.prnewswire.com/news-releases/equifax-announces-cybersecurity-incident-involving-consumer-information-300515960.html (last visited September 13, 2017).

[2] *Id.*

24. Moreover, Plaintiff has a continuing interest in ensuring that his Personal Information, which remains in the possession of Equifax, is protected and safeguarded from future breaches.

25. At all relevant times, Equifax was well aware, or reasonably should have been aware, that the Personal Information it collected, maintained, and stored is highly sensitive, susceptible to attack, and could be used for wrongful purposes, such as identify theft and fraud, by third parties.

26. It is well known and the subject of many media reports that Personal Information is highly coveted and a frequent target of hackers. Despite the frequent public announcements of data breaches of corporate entities, including Experian, Equifax maintained an insufficient and inadequate system to protect the Personal Information of Plaintiff and Class members.

27. Personal Information is a valuable commodity because it contains not only payment card numbers but personal data as well. A cyber black market exists in which criminals openly post stolen payment card numbers, Social Security numbers, and other personal information on a number of underground Internet websites. Personal Information is valuable to identity thieves because they can use victims' personal data to open new financial accounts and take out loans in another person's name, incur charges on existing accounts, or clone ATM, debit, or credit cards.

28. Legitimate organizations and the criminal underground alike recognize the value in Personal Information contained in a merchant's data systems; otherwise, they would not aggressively seek or pay for it. For example, in "[o]ne of 2013's largest breaches," "[n]ot only

did hackers compromise the [card holder data] of three million customers, they also took registration data [containing Personal Information] from 38 million users."[3]

29. At all relevant times, Equifax knew, or reasonably should have known, of the importance of safeguarding Personal Information and of the foreseeable consequences that would occur if its data security system was breached, including, specifically, the significant costs that would be imposed on individuals as a result of a breach.

30. Equifax was, or should have been, fully aware of the significant number of people whose Personal Information it collected and, thus, the significant number of individuals who would be harmed by a breach of Equifax's systems.

31. Despite all of this publicly available knowledge of the continued compromises of Personal Information in the hands of other third parties, Equifax's approach to maintaining the privacy and security of the Personal Information of Plaintiff and Class members was reckless or, at the very least, negligent.

32. The ramifications of Equifax's failure to keep Plaintiff's and Class members' data secure are severe.

33. The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[4] The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including a person's name, Social Security number, and date of birth.[5]

---

[3] Verizon 2014 PCI Compliance Report at 54, available at: https://www.cisco.com/c/dam/en_us/solutions/industries/docs/retail/verizon_pci2014.pdf (last visited September 14, 2017).

[4] 17 C.F.R. § 248.201(b)(9).

[5] 17 C.F.R. § 248.201(b)(8).

34. Personal Information is a valuable commodity to identity thieves once the information has been compromised. As the FTC recognizes, once identity thieves have personal information, "they can drain your bank account, run up your credit cards, open new utility accounts, or get medical treatment on your health insurance."[6]

35. Identity thieves can use personal information, such as the Personal Information of Plaintiff and Class members which Equifax failed to keep secure, to perpetrate a variety of crimes that harm victims. For instance, identity thieves may commit various types of government fraud such as immigration fraud; obtaining a driver's license or identification card in the victim's name but with another's picture; using the victim's information to obtain government benefits; or filing a fraudulent tax return using the victim's information to obtain a fraudulent refund.

36. In 2016, Javelin Strategy and Research reported that identity thieves stole $112 billion in the previous six years.[7]

37. Reimbursing a consumer for a financial loss due to fraud does not make that individual whole again. On the contrary, identity theft victims must spend numerous hours and their own money repairing the impact to their credit. After conducting a study, the Department of Justice's Bureau of Justice Statistics found that identity theft victims "reported spending an average of about 7 hours clearing up the issues" and resolving the consequences of fraud in 2014.[8]

---

6 Federal Trade Commission, Warning Signs of Identity Theft, available at: https://www.consumer.ftc.gov/articles/0271-warning-signs-identity-theft (last visited September 14, 2017).

7 See https://www.javelinstrategy.com/coverage-area/2016-identity-fraud-fraud-hits-inflection-point (last visited September 14, 2017).

8 Victims of Identity Theft, 2014 at 10 (Sept. 2015), available at: https://www.bjs.gov/content/pub/pdf/vit14.pdf (last visited September 14, 2017).

38. There may be a time lag between when harm occurs versus when it is discovered, and also between when Personal Information is stolen and when it is used. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[9]

39. Plaintiff and Class members now face years of constant surveillance and monitoring of their financial and personal records and losses of benefits and rights. The Class is incurring and will continue to incur such damages in addition to any fraudulent use of their Personal Information.

40. The Personal Information of Plaintiff and Class members is private and sensitive in nature and was left inadequately protected by Equifax. Equifax did not obtain Plaintiff's and Class members' consent to disclose their Personal Information to any other person as required by applicable law and industry standards.

41. The Equifax Data Breach was a direct and proximate result of Equifax's failure to properly safeguard and protect Plaintiff's and Class members' Personal Information from unauthorized access, use, and disclosure, as required by various state and federal regulations, industry practices, and the common law, including Equifax's failure to establish and implement appropriate administrative, technical, and physical safeguards to ensure the security and

[9] GAO, Report to Congressional Requesters, at 29 (June 2007), available at: http://www.gao.gov/new.items/d07737.pdf (last visited September 14, 2017).

confidentiality of Plaintiff's and Class members' Personal Information to protect against reasonably foreseeable threats to the security or integrity of such information.

42. Equifax had the resources to prevent a breach, but it neglected to adequately invest in data security, despite the growing number of well-publicized data breaches.

43. Had Equifax remedied the deficiencies in its data security systems, followed security guidelines, and adopted adequate security measures, Equifax would have prevented the Data Breach and, ultimately, the theft of its customers' Personal Information.

44. As a direct and proximate result of Equifax's wrongful actions and inaction and the resulting Data Breach, Plaintiff and Class members have been placed at an imminent, immediate, and continuing increased risk of harm from identity theft and identity fraud, requiring them to take the time which they otherwise would have dedicated to other life demands such as work to mitigate the actual and potential impact of the Data Breach on their lives including, among other things, by placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, closely reviewing and monitoring their credit reports and accounts for unauthorized activity, and filing police reports. This time has been lost forever and cannot be recaptured. In all manners of life in this country, time has constantly been recognized as compensable; for many consumers, it is the way they are compensated, and even if retired from the work force, consumers should be free of having to deal with the consequences of a credit reporting agency's negligence, as is the case here.

45. Equifax's wrongful actions and inaction directly and proximately caused the theft and dissemination into the public domain of Plaintiff's and Class members' Personal Information, causing them to suffer, and continue to suffer, economic damages and other actual harm for which they are entitled to compensation, including:

a. theft of their personal and financial information;

b. unauthorized charges on their debit and credit card accounts;

c. the imminent and certainly impending injury flowing from potential fraud and identity theft posed by their Personal Information being placed in the hands of criminals and already misused via the sale of Plaintiff's and Class members' information on the black market;

d. the untimely and inadequate notification of the Data Breach;

e. the improper disclosure of their Personal Information;

f. loss of privacy;

g. ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach;

h. ascertainable losses in the form of deprivation of the value of their Personal Information, for which there is a well-established national and international market;

i. ascertainable losses in the form of the loss of cash-back or other benefits as a result of their inability to use certain accounts and cards affected by the Data Breach;

j. loss of use of and access to their account funds and costs associated with the inability to obtain money from their accounts or being limited in the amount of money they were permitted to obtain from their accounts, including missed payments on bills and loans, late charges and fees, and adverse effects on their credit including adverse credit notations; and,

k. the loss of productivity and value of their time spent to address attempt to ameliorate, mitigate and deal with the actual and future consequences of the data breach, including finding fraudulent charges, cancelling and reissuing cards, purchasing credit monitoring and identity theft protection services, imposition of withdrawal and purchase limits on compromised accounts, and the stress, nuisance and annoyance of dealing with all such issues resulting from the Data Breach.

46. While the Personal Information of Plaintiff and members of the Class has been stolen, Equifax continues to hold Personal Information of consumers, including Plaintiff and Class members. Particularly because Equifax has demonstrated an inability to prevent a breach

or stop it from continuing even after being detected, Plaintiff and members of the Class have an undeniable interest in insuring that their Personal Information is secure, remains secure, is properly and promptly destroyed and is not subject to further theft.

CLASS ACTION ALLEGATIONS

47. Plaintiff seeks relief on behalf of himself and as representatives of all others who are similarly situated. Pursuant to Fed. R. Civ. P. 23(a), (b)(2), (b)(3) and (c)(4), Plaintiff seeks certification of a "Nationwide Class" defined as follows:

> All persons residing in the United States whose personally identifiable information was acquired by unauthorized persons in the data breach announced by Equifax in September 2017.

48. Alternatively, pursuant to Fed. R. Civ. P. 23, Plaintiff assert claims under the laws of Tennessee and on behalf of separate "Tennessee Class," defined as follows:

> All persons residing in Tennessee as of the date of this filing whose personally identifiable information was acquired by unauthorized persons in the data breach announced by Equifax in September 2017.

49. Excluded from each of the above Classes are Equifax and any of its affiliates, parents, or subsidiaries; all employees of Equifax; all persons who make a timely election to be excluded from the Class; government entities; class counsel; and the judges to whom this case is assigned and their immediate family and court staff.

50. Plaintiff hereby reserves the right to amend or modify the class definition with greater specificity or division after having had an opportunity to conduct discovery.

51. Each of the proposed Classes meets the criteria for certification under Federal Rule of Civil Procedure 23(a), (b)(2), (b)(3) and (c)(4).

52. Numerosity - Fed. R. Civ. P. 23(a)(1). Consistent with Rule 23(a)(1), the members of the Class are so numerous and geographically dispersed that the joinder of all

members is impractical. While the exact number of Class members is unknown to Plaintiff at this time, the proposed Class includes potentially 143 million individuals whose Personal Information was compromised in the Equifax Data Breach. Class members may be identified through objective means. Class members may be notified of the pendency of this action by recognized, Court-approved notice dissemination methods, which may include U.S. mail, electronic mail, internet postings, and/or published notice.

53. Commonality - Fed. R. Civ. P. 23(a)(2) and (b)(3). Consistent with Fed. R. Civ. P. 23(a)(2) and with 23(b)(3)'s predominance requirement, this action involves common questions of law and fact that predominate over any questions affecting individual Class members. The common questions include:

a. Whether Equifax had a duty to protect Personal Information;

b. Whether Equifax knew or should have known of the susceptibility of their data security systems to a data breach;

c. Whether Equifax's security measures to protect their systems were reasonable;

d. Whether Equifax was negligent in failing to implement reasonable and adequate security procedures and practices;

e. Whether Equifax's failure to implement adequate data security measures allowed the breach to occur;

f. Whether Equifax's conduct, including their failure to act, resulted in or was the proximate cause of the breach of its systems, resulting in the loss of the Personal Information of Plaintiff and Class members;

g. Whether Plaintiff and Class members were injured and suffered damages or other acceptable losses because of Equifax's failure to reasonably protect its POS systems and data network; and

h. Whether Plaintiff and Class members are entitled to relief.

54. Typicality - Fed. R. Civ. P. 23(a)(3). Consistent with Fed. R. Civ. P. 23(a)(3), Plaintiff's claims are typical of those of other Class members. Plaintiff had his Personal Information compromised in the Data Breach. Plaintiff's damages and injuries are akin to other Class members and Plaintiff seeks relief consistent with the relief of the Class.

55. Adequacy - Fed. R. Civ. P. 23(a)(4). Consistent with Fed. R. Civ. P. 23(a)(4), Plaintiff is an adequate representative of the Class because Plaintiff is a member of the Class and is committed to pursuing this matter against Equifax to obtain relief for the Class. Plaintiff has no conflicts of interest with the Class. Plaintiff's Counsel are competent and experienced in litigating class actions, including privacy litigation. Plaintiff intends to vigorously prosecute this case and will fairly and adequately protect the Class' interests.

56. Superiority - Fed. R. Civ. P. 23(b)(3). Consistent with Fed. R. Civ. P 23(b)(3), a class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this class action. The quintessential purpose of the class action mechanism is to permit litigation against wrongdoers even when damages to individual plaintiffs may not be sufficient to justify individual litigation. Here, the damages suffered by Plaintiff and the Class are relatively small compared to the burden and expense required to individually litigate their claims against Equifax, and thus, individual litigation to redress Equifax's wrongful conduct would be impracticable. Individual litigation by each Class member would also strain the court system. Individual litigation creates the potential for inconsistent or contradictory judgments and increases the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties and provides the benefits of a single adjudication, economies of scale, and comprehensive supervision by a single court.

57. Injunctive and Declaratory Relief. Class certification is also appropriate under Fed. R. Civ. P. 23(b)(2) and (c). Defendant, through its uniform conduct, has acted or refused to act on grounds generally applicable to the Class as a whole, making injunctive and declaratory relief appropriate to the Class as a whole.

58. Likewise, particular issues under Rule 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. Whether Equifax failed to timely notify the public of the Data Breach;

b. Whether Equifax owed a legal duty to Plaintiff and the Class to exercise due care in collecting, storing, and safeguarding their Personal Information;

c. Whether Equifax's security measures were reasonable in light of data security recommendations, and other measures recommended by data security experts;

d. Whether Equifax failed to adequately comply with industry standards amounting to negligence;

e. Whether Defendant failed to take commercially reasonable steps to safeguard the Personal Information of Plaintiff and the Class members; and

f. Whether adherence to data security recommendations, and measures would have reasonably prevented the Data Breach.

59. Finally, all members of the proposed Classes are readily ascertainable. Equifax has access to information regarding the Data Breach, the time period of the Data Breach, and which individuals were potentially affected. Using this information, the members of the Class can be identified and their contact information ascertained for purposes of providing notice to the Class.

CLAIMS FOR RELIEF

COUNT I

NEGLIGENCE

60. Plaintiff restates and realleges Paragraphs 1 through 59 as if fully set forth herein.

61. Upon accepting and storing the Personal Information of Plaintiff and Class members in its computer systems and on its networks, Equifax undertook and owed a duty to Plaintiff and Class members to exercise reasonable care to secure and safeguard that information and to use commercially reasonable methods to do so. Equifax knew that the Personal Information was private and confidential and should be protected as private and confidential.

62. Equifax owed a duty of care not to subject Plaintiff and Class members, along with their Personal Information, to an unreasonable risk of harm because they were foreseeable and probable victims of any inadequate security practices.

63. Equifax owed numerous duties to Plaintiff and to members of the Class, including the following:

a. To exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting and protecting Personal Information in its possession;

b. To protect Personal Information using reasonable and adequate security procedures and systems that are compliant with industry-standard practices; and

c. To implement processes to quickly detect a data breach and to timely act on warnings about data breaches.

64. Equifax also breached its duty to Plaintiff and the Class members to adequately protect and safeguard Personal Information by knowingly disregarding standard information-security principles, despite obvious risks, and by allowing unmonitored and unrestricted access to unsecured Personal Information. Furthering their dilatory practices, Equifax failed to provide

adequate supervision and oversight of the Personal Information with which they were and are entrusted, in spite of the known risk and foreseeable likelihood of breach and misuse, which permitted an unknown third party to gather Personal Information of Plaintiff and Class members, misuse the Personal Information, and intentionally disclose it to others without consent.

65. Equifax knew, or should have known, of the risks inherent in collecting and storing Personal Information, the vulnerabilities of its data security systems, and the importance of adequate security. Equifax knew about numerous, well-publicized data breaches, including the breach at Experian.

66. Equifax knew, or should have known, that its data systems and networks did not adequately safeguard Plaintiff's and Class members' Personal Information.

67. Equifax breached its duties to Plaintiff and Class members by failing to provide fair, reasonable, or adequate computer systems, and data-security practices to safeguard Personal Information of Plaintiff and Class members.

68. Because Equifax knew that a breach of its systems would damage millions of individuals, including Plaintiff and Class members, Equifax had a duty to adequately protect its data systems and the Personal Information contained thereon.

69. Equifax had a special relationship with Plaintiff and Class members.

70. Plaintiff's and Class members' willingness to entrust Equifax with their Personal Information was predicated on the understanding that Equifax would take adequate security precautions. Moreover, only Equifax had the ability to protect its systems and the Personal Information it stored on them from attack.

71. Equifax's own conduct also created a foreseeable risk of harm to Plaintiff and Class members and their Personal Information. Equifax's misconduct included failing to: (1)

secure its systems, despite knowing their vulnerabilities, (2) comply with industry-standard security practices, (3) implement adequate system and event monitoring, and (4) implement the systems, policies, and procedures necessary to prevent this type of data breach.

72. Equifax also had independent duties under state and federal laws that required Equifax to reasonably safeguard Plaintiff's and Class members' Personal Information and promptly notify them about the Data Breach.

73. Equifax breached its duties to Plaintiff and Class members in numerous ways, including:

a. by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Personal Information of Plaintiff and Class members;

b. by creating a foreseeable risk of harm through the misconduct previously described;

c. by failing to implement adequate security systems, protocols and practices sufficient to protect Plaintiff's and Class members' Personal Information both before and after learning of the Data Breach;

d. by failing to comply with the minimum industry data-security standards during the period of the Data Breach; and

e. by failing to timely and accurately disclose that Plaintiff's and Class members' Personal Information had been improperly acquired or accessed.

74. Through Equifax's acts and omissions described in this Complaint, including Equifax's failure to provide adequate security and its failure to protect Personal Information of Plaintiff and Class members from being foreseeably captured, accessed, disseminated, stolen, and misused, Equifax unlawfully breached its duty to use reasonable care to adequately protect and secure Personal Information of Plaintiff and Class members during the time it was within Equifax's possession or control.

75. The law further imposes an affirmative duty on Equifax to timely disclose the unauthorized access and theft of the Personal Information to Plaintiff and the Class so that Plaintiff and Class members can take appropriate measures to mitigate damages, protect against adverse consequences, and thwart future misuse of their Personal Information.

76. Equifax breached its duty to notify Plaintiff and Class members of the unauthorized access by waiting weeks after learning of the breach to notify Plaintiff and Class members and then by failing to provide Plaintiff and Class members information regarding the breach until September 2017. Instead, its executives disposed of at least $1.8 million worth of shares in the company after Equifax learned of the data breach but before it was publicly announced. To date, Equifax has not provided sufficient information to Plaintiff and Class members regarding the extent of the unauthorized access and continues to breach its disclosure obligations to Plaintiff and the Class.

77. Further, through its failure to provide timely and clear notification of the Data Breach to consumers, Equifax prevented Plaintiff and Class members from taking meaningful, proactive steps to secure their financial data and bank accounts.

78. Upon information and belief, Equifax improperly and inadequately safeguarded Personal Information of Plaintiff and Class members in deviation of standard industry rules, regulations, and practices at the time of the unauthorized access. Equifax's failure to take proper security measures to protect sensitive Personal Information of Plaintiff and Class members as described in this Complaint, created conditions conducive to a foreseeable, intentional criminal act, namely the unauthorized access of Personal Information of Plaintiff and Class members.

79. Equifax's conduct was grossly negligent and departed from all reasonable standards of care, including, but not limited to: failing to adequately protect the Personal

Information; failing to conduct regular security audits; failing to provide adequate and appropriate supervision of persons having access to Personal Information of Plaintiff and Class members; and failing to provide Plaintiff and Class members with timely and sufficient notice that their sensitive Personal Information had been compromised.

80. Neither Plaintiff nor the other Class members contributed to the Data Breach and subsequent misuse of their Personal Information as described in this Complaint.

81. As a direct and proximate cause of Equifax's conduct, Plaintiff and the Class members suffered damages including, but not limited to, damages arising from the unauthorized charges on their debit or credit cards or on cards that were fraudulently obtained through the use of the Personal Information of Plaintiff and Class members; damages arising from Plaintiff's inability to use their debit or credit cards because those cards were cancelled, suspended, or otherwise rendered unusable as a result of the Data Breach and/or false or fraudulent charges stemming from the Data Breach, including but not limited to late fees charges and foregone cash-back and other rewards; damages from lost time and effort to mitigate the actual and potential impact of the Data Breach on their lives including, among other things, by placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, closely reviewing and monitoring their credit reports and accounts for unauthorized activity, and filing police reports and damages from identity theft, which may take months if not years to discover and detect, given the far-reaching, adverse, and detrimental consequences of identity theft and loss of privacy. The nature of other forms of economic damage and injury may take years to detect, and the potential scope can only be assessed after a thorough investigation of the facts and events surrounding the theft mentioned above.

COUNT II

NEGLIGENCE *PER SE*

82. Plaintiff restates and realleges Paragraphs 1 through 81 as if fully set forth herein.

83. The Federal Trade Commission Act ("FTCA"), codified at 15 U.S.C. § 41 *et seq*., prohibits "unfair . . . acts or practices in or affecting commerce." FTCA § 5, 15 U.S.C. § 45. As interpreted and enforced by the FTC, such unfair acts or practices include the unfair acts or practices by businesses, such as Equifax, of failing to use reasonable measures to protect Personal Information. The FTC publications and orders described in this Complaint also form part of the basis of Equifax's duty in this regard.

84. Equifax violated 15 U.S.C. § 45 by failing to use reasonable measures to protect Personal Information and not complying with applicable industry standards, as described in detail herein. Equifax's conduct was particularly unreasonable given the nature and amount of Personal Information it obtained and stored, and the foreseeable consequences of a data breach at a corporation such as Equifax, including, specifically, the immense damages that would result to Plaintiff and Class members.

85. Equifax's violation 15 U.S.C. § 45 constitutes negligence *per se*.

86. Plaintiff and Class members are within the class of persons that the FTCA was intended to protect.

87. The harm that occurred as a result of the Equifax Data Breach is the type of harm the FTCA was intended to guard against. The FTC has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and the Class members.

88. As a direct and proximate result of Equifax's negligence *per se*, Plaintiff and the Class members have suffered, and continue to suffer, injuries and damages arising from Plaintiff's inability to use their debit or credit cards because those cards were cancelled, suspended, or otherwise rendered unusable as a result of the Data Breach and/or false or fraudulent charges stemming from the Data Breach, including but not limited to late fees charges and foregone cash-back and other rewards; damages from lost time and effort to mitigate the actual and potential impact of the Data Breach on their lives including, inter alia, by placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, closely reviewing and monitoring their credit reports and accounts for unauthorized activity, and filing police reports and damages from identity theft, which may take months if not years to discover and detect, given the far-reaching, adverse, and detrimental consequences of identity theft and loss of privacy.

COUNT III

WILLFUL VIOLATION OF THE FAIR CREDIT REPORTING ACT

89. Plaintiff restates and realleges Paragraphs 1 through 88 as if fully set forth here.

90. As individuals, Plaintiff and Class member are "consumers" entitled to the protections of the Fair Credit Reporting Act ("FCRA") 15 U.S.C. § 1681a(c).

91. Under the FCRA, a "consumer reporting agency" is defined as "any person which, for monetary fees, dues, or on a cooperative nonprofit basis, regularly engages in whole or in part in the practice of assembling or evaluating consumer credit information or other information on consumers for the purpose of furnishing consumer reports to third parties . . . ." 15 U.S.C. § 1681a(f).

92. Equifax is a consumer reporting agency under the FCRA.

93. As a consumer reporting agency, the FCRA requires Equifax to "maintain reasonable procedures designed to . . . limit the furnishing of consumer reports to the purposes listed under section 1681b of this title." 15 U.S.C. § 1681e(a).

94. Under the FCRA, a "consumer report" is defined as "any written, oral, or other communication of any information by a consumer reporting agency bearing on a consumer's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living which is used or expected to be used or collected in whole or in part for the purpose of serving as a factor in establishing the consumer's eligibility for -- (A) credit . . . to be used primarily for personal, family, or household purposes; . . . or (C) any other purpose authorized under section 1681b of this title." 15 U.S.C. § 1681a(d)(1). The compromised data, including Plaintiff's and Class members' Personal Information, was a consumer report under the FCRA.

95. As a consumer reporting agency, Equifax may only furnish a consumer report under the limited circumstances set forth in 15 U.S.C. § 1681b, "and no other." 15 U.S.C. § 1681b(a). None of the purposes listed under 15 U.S.C. § 1681b permit credit reporting agencies to furnish consumer reports to unauthorized or unknown entities, or computer hackers such as those who accessed Plaintiff's and the Class members' Personal Information. Equifax violated § 1681b by furnishing consumer reports to unauthorized or unknown entities or computer hackers, as detailed above.

96. Equifax furnished Plaintiff's and Class members' consumer reports by disclosing their consumer reports to unauthorized entities and computer hackers; allowing unauthorized entities and computer hackers to access their consumer reports; knowingly and/or recklessly failing to take security measures that would prevent unauthorized entities or computer hackers

from accessing their consumer reports; and/or failing to take reasonable security measures that would prevent unauthorized entities or computer hackers from accessing their consumer reports.

97. The FTC has pursued enforcement actions against consumer reporting agencies under the FCRA for failing to "take adequate measures to fulfill their obligations to protect information contained in consumer reports, as required by the" FCRA, in connection with data breaches. *In the Matter of SettlementOne Credit Corp.*, FTC Docket No. C-4330, 2011 WL 3726287, at *10 (August 17, 2011).

98. Equifax willfully and/or recklessly violated § 1681b and § 1681e(a) by providing impermissible access to consumer reports and by failing to maintain reasonable procedures designed to limit the furnishing of consumer reports to the purposes outlined under § 1681b of the FCRA. The willful and reckless nature of Equifax's violations is supported by, among other things, former employees' admissions that Equifax's data security practices have deteriorated in recent years, and Equifax's numerous other data breaches in the past. Further, Equifax touts itself as an industry leader in breach prevention; thus, Equifax was well aware of the importance of the measures organizations should take to prevent data breaches, and willingly failed to take them.

99. Equifax also acted willfully and recklessly because it knew or should have known about its legal obligations regarding data security and data breaches under the FCRA. These obligations are well established in the plain language of the FCRA and in the promulgations of the Federal Trade Commission. *See, e.g.*, Statement of General Policy or Interpretation; Commentary on the Fair Credit Reporting Act, 55 Fed. Reg. 18804, 1990 WL 342991 (May 4, 1990). Equifax obtained or had available these and other substantial written materials that apprised them of their duties under the FCRA. Any reasonable consumer reporting agency knows or should know about these requirements. Despite knowing of these legal obligations,

Equifax acted consciously in breaching known duties regarding data security and data breaches and depriving Plaintiff and Class members of their rights under the FCRA.

100. Equifax's willful and/or reckless conduct provided a means for unauthorized intruders to obtain and misuse Plaintiff's and Class members' personal information for no permissible purposes under the FCRA.

101. Plaintiff and Class members have been damaged by Equifax's willful or reckless failure to comply with the FCRA. Therefore, Plaintiff and each of the Class members are entitled to recover "any actual damages sustained by the consumer . . . or damages of not less than $100 and not more than $1,000." 15 U.S.C. § 1681n(a)(1)(A).

102. Plaintiff and Class members are also entitled to punitive damages, costs of the action, and reasonable attorneys' fees. 15 U.S.C. § 1681n(a)(2) & (3).

COUNT IV

NEGLIGENT VIOLATION OF THE FAIR CREDIT REPORTING ACT

103. Plaintiff restates and realleges Paragraphs 1 through 102 as if fully set forth herein.

104. Equifax was negligent in failing to maintain reasonable procedures designed to limit the furnishing of consumer reports to the purposes outlined under section 1681b of the FCRA. Equifax's negligent failure to maintain reasonable procedures is supported by, among other things, former employees' admissions that Equifax's data security practices have deteriorated in recent years, and Equifax's numerous other data breaches in the past. Further, as an enterprise claiming to be an industry leader in data breach prevention, Equifax was well aware of the importance of the measures organizations should take to prevent data breaches, yet failed to take them.

105. Equifax's negligent conduct provided a means for unauthorized intruders to obtain Plaintiff's and Class members' Personal Information and consumer reports for no permissible purposes under the FCRA.

106. Plaintiff and Class member have been damaged by Equifax's negligent failure to comply with the FCRA. Therefore, Plaintiff and Class members are entitled to recover "any actual damages sustained by the consumer." 15 U.S.C. § 1681o(a)(1).

107. Plaintiff and Class members are also entitled to recover their costs of the action, as well as reasonable attorneys' fees. 15 U.S.C. § 1681o(a)(2).

COUNT V

DECLARATORY JUDGMENT

108. Plaintiff restates and realleges Paragraphs 1 through 107 as if fully set forth herein.

109. As previously alleged, Plaintiff and Class members entered into an implied contract that required Equifax to provide adequate security for the Personal Information it collected from their payment card transactions. As previously alleged, Equifax owes duties of care to Plaintiff and Class members that require it to adequately secure Personal Information.

110. Equifax still possesses Personal Information pertaining to Plaintiff and Class members.

111. Equifax has made no announcement or notification that it has remedied the vulnerabilities in its computer data systems, and, most importantly, its systems.

112. Accordingly, Equifax has not satisfied its contractual obligations and legal duties to Plaintiff and Class members. In fact, now that Equifax's lax approach towards data security

has become public, the Personal Information in its possession is more vulnerable than it was previously.

113. Actual harm has arisen in the wake of the Equifax Data Breach regarding Equifax's contractual obligations and duties of care to provide data security measures to Plaintiff and Class members.

114. Plaintiff seeks a declaration that (a) Equifax's existing data security measures do not comply with its contractual obligations and duties of care, and (b) in order to comply with its contractual obligations and duties of care, Equifax must implement and maintain reasonable security measures, including, but not limited to:

a. engaging third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Equifax's systems on a periodic basis, and ordering Equifax to promptly correct any problems or issues detected by such third-party security auditors;

b. engaging third-party security auditors and internal personnel to run automated security monitoring;

c. auditing, testing, and training its security personnel regarding any new or modified procedures;

d. segmenting Personal Information by, among other things, creating firewalls and access controls so that if one area of Equifax is compromised, hackers cannot gain access to other portions of Equifax systems;

e. purging, deleting, and destroying in a reasonable secure manner Personal Information not necessary for its provisions of services;

f. conducting regular database scanning and securing checks;

g. routinely and continually conducting internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach; and

h. educating its customers about the threats they face as a result of the loss of their financial and personal information to third parties, as well as the steps Equifax customers must take to protect themselves.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, individually and on behalf of all Class members proposed in this Complaint, prays as follows:

a. For an Order certifying the Nationwide Class or, alternatively, the Tennessee Class, as defined herein, and appointing Plaintiff as Class representative and his attorneys as Class counsel;

b. For a declaration that Equifax's data security measures do not comply with its contractual obligations and duties of care;

c. For equitable relief enjoining Equifax from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiff's and Class members' Personal Information, and from refusing to issue prompt, complete, and accurate disclosures to the Plaintiff and Class members;

d. For equitable relief compelling Equifax to use appropriate cyber-security methods and policies with respect to consumer data collection, storage, and protection and to disclose with specificity to Plaintiff and Class members the type of Personal Information compromised;

e. For damages, as allowed by law in an amount to be determined;

f. For an award of attorneys' fees, costs, and litigation expenses, as allowable by law;

g. For prejudgment interest on all amounts awarded; and

h. For such other and further relief as this Court may deem just and proper.

JURY DEMAND

Plaintiff demands a jury trial on all issues so triable.

Dated: September 15, 2017.

Respectfully submitted,

/s/ *Charles Barrett*

Charles Barrett, BPR # 020627
Benjamin C. Aaron, BPR #034118
NEAL & HARWELL, PLC
1201 Demonbreun St.
Suite 1000
Nashville, TN 37203
(615) 244-1713
cbarrett@nealharwell.com
baaron@nealharwell.com

Don Barrett
David McMullan, Jr.
Sterling Starnes
Cary Littlejohn
DON BARRETT, P.A.
404 Court Square North
Lexington, MS 39095
(662) 834-2488
dbarrett@barrettlawgroup.com
dmcmullan@barrettlawgroup.com
sstarnes@barrettlawgroup.com
clittlejohn@barrettlawgroup.com

Roberta D. Liebenberg
Gerard A. Dever
Adam J. Pessin
FINE, KAPLAN AND BLACK, R.P.C.
One S. Broad Street, 23rd Floor
Philadelphia, PA 19107
(215) 567-6565
rliebenberg@finekaplan.com
gdever@finekaplan.com
apessin@finekaplan.com